

RON WYDEN
OREGON

CHAIRMAN OF COMMITTEE ON
FINANCE

221 DIRKSEN SENATE OFFICE BUILDING
WASHINGTON, DC 20510
(202) 224-5244

United States Senate
WASHINGTON, DC 20510-3703

COMMITTEES:
COMMITTEE ON FINANCE
COMMITTEE ON THE BUDGET
COMMITTEE ON ENERGY AND NATURAL RESOURCES
SELECT COMMITTEE ON INTELLIGENCE
JOINT COMMITTEE ON TAXATION

May 6, 2025

The Honorable Pam Bondi
Attorney General
Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530

Dear Attorney General Bondi:

I write to request that the Department of Justice (DOJ) investigate the serious threat to U.S. national security posed by TeleMessage, a federal contractor that sold dangerously insecure communications software to the White House and other federal agencies.

Communications from several federal agencies, including the most senior national security officials, have been recklessly entrusted to TeleMessage, a foreign company that purports to offer agencies a secure tool to archive messages sent using Signal, the popular secure messaging app. A photo published by Reuters last week revealed that then-national security advisor Mike Waltz uses TeleMessage Signal Archiver (“TeleMessage Archiver”). The photo, captured at a cabinet meeting, showed that he was using the app to communicate with other senior officials, including Vice President J.D. Vance, Director of National Intelligence Tulsi Gabbard, and Secretary of State Marco Rubio, who has since also been made the national security advisor.

TeleMessage Archiver is a modified version of Signal that looks the same as Signal and can be used to communicate with other Signal users. The White House seemingly adopted TeleMessage Archiver in the wake of the “Signalgate” scandal earlier this year, after Waltz accidentally added a journalist to a group chat in which classified information was shared. Screenshots published by The Atlantic revealed that the Signalgate group chat had been configured by Waltz to auto-erase messages, likely in violation of federal recordkeeping laws. Reminded of its obligation to retain officials’ text chats by several lawsuits, it appears that the White House equipped Waltz with TeleMessage Archiver.

Signal encrypts all messages using a security method known as end-to-end encryption, which ensures that messages are only accessible to the conversation participants and not to third parties,

911 NE 11TH AVENUE
SUITE 630
PORTLAND, OR 97232
(503) 326-7525

405 EAST 8TH AVE
SUITE 2020
EUGENE, OR 97401
(541) 431-0229

SAC ANNEX BUILDING
105 FIR ST
SUITE 201
LA GRANDE, OR 97850
(541) 962-7691

U.S. COURTHOUSE
310 WEST 6TH ST
ROOM 118
MEDFORD, OR 97501
(541) 858-5122

THE JAMISON BUILDING
131 NW HAWTHORNE AVE
SUITE 107
BEND, OR 97701
(541) 330-9142

707 13TH ST, SE
SUITE 285
SALEM, OR 97301
(503) 589-4555

[HTTPS://WYDEN.SENATE.GOV](https://wyden.senate.gov)

PRINTED ON RECYCLED PAPER

including the service provider. End-to-end encryption is the gold standard for encryption, because user communications remain secure even if a service provider's server is hacked. In its marketing materials, TeleMessage has claimed that it secures its customers' communications with end-to-end encryption. Indeed, an executive at TeleMessage's parent company, Smarsh, told the New York Times last week that information was not decrypted while being collected for record-keeping purposes or moved to its final archive, stating that "We do not de-encrypt." These claims are plainly false. A prominent cybersecurity expert recently published their own analysis of the app, based on TeleMessage Archiver's source code, which the company published on its website. This researcher determined that the app sends a copy of every message sent or received by a user back to a server administered by the company, before they are then delivered to the user's employer for retention. As such, each message is seemingly accessible to the company, or anyone else that has access to its server.

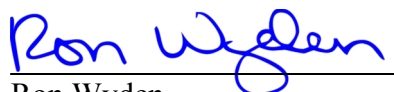
The government agencies that have adopted TeleMessage Archiver have chosen the worst possible option. They have given their users something that looks and feels like Signal, the most widely trusted secure communications app. But instead, senior government officials have been provided with a shoddy Signal knockoff that poses a number of serious security and counterintelligence threats. The security threat posed by TeleMessage Archiver is not theoretical. Over the past couple days, at least two different hackers discovered and exploited vulnerabilities in the company's systems. On May 4, 2025, 404 Media reported that a hacker discovered and exploited a vulnerability in TeleMessage's server, enabling them to gain access to the communications and other data of TeleMessage customers, including employees of U.S. Customs and Border Protection (CBP). The hacker told the press that "I would say the whole process took about 15-20 minutes...It wasn't much effort at all." On May 5, 2025, NBC News reported that a different hacker also broke into the company's server and stole a "large cache of files." After that second hack, the company suspended all of its services.

The underlying problem is that agencies want to be able to retain communications of employees using an app that was not designed around that requirement. Signal is designed for regular users, who do not need nor want their messages to be kept forever, let alone archived on a central server. Tacking record retention capabilities onto Signal without significantly undermining its security was always going to be difficult. Moreover, TeleMessage appears to have designed the feature in a way that succeeds only in introducing new vulnerabilities. It would be hard to imagine a less secure way for U.S. government agencies to retain employee messages than decrypting, copying to, and processing those messages on a poorly secured server operated by a foreign company. It remains unclear whether the design of this system was merely the result of incompetence on the part of the foreign company, whose senior leadership are former intelligence officers, or a backdoor designed to facilitate foreign intelligence collection against U.S. government officials. Regardless, TeleMessage's dangerously insecure design should have been discovered long before the company's app was installed on the phone of the President's national security advisor and, presumably, other senior White House officials.

The government's use of TeleMessage Archiver seriously threatens U.S. national security, which I urge you to investigate. First, TeleMessage appears to have misled the federal government about the security of its products, including by claiming to provide end-to-end encryption when it does not. TeleMessage certainly would not have obtained its federal contracts if agencies knew how shoddy its security practices really were and because its claims were false, at least two hackers were able to gain access to communications and other data from federal customers, including employees of CBP. TeleMessage must be held accountable for its apparent false statements to federal agencies and for its apparent violations of the cybersecurity requirements in federal contracts. I urge the DOJ to investigate whether TeleMessage violated the False Claims Act by selling insecure products to the federal government. Second, I urge you to launch an investigation into the counterintelligence threat posed by TeleMessage, to determine the extent to which foreign employees of the company have access to the messages of government users, whether the company has shared U.S. government communications with the Israeli government, and whether the Israeli government played any role in the product's dangerous design.

Thank you for your attention to this important matter. If you have any questions about this request, please contact Chris Soghoian in my office.

Sincerely,



Ron Wyden
Ron Wyden
United States Senator

Cc:

The Honorable Tulsi Gabbard, Director of National Intelligence.

The Honorable Andrew N. Ferguson, Chairman, Federal Trade Commission.

The Honorable Joseph Joseph Cuffari, Inspector General, Department of Homeland Security.

Mr. Gregory Barbaccia, Federal Chief Information Officer, Office of Management and Budget.